Notice of Allowability	Application No. 09/651,303	Applicant(s) MORAN, DOUGLAS B.	
	Examiner Ronald Baum	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *10/21/2004*.

2. ☒ The allowed claim(s) is/are *1,2,5,9-17 and 19-23*.

3. ☒ The drawings filed on 8/30/00 are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

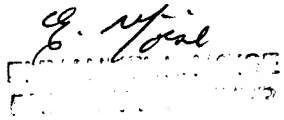
6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *12232004* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.



EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with William J. James, Reg. No. 40,661 on 12/15/2004.

1. Replace claims 1,9,10,22,23 with:

1. A system for detecting intrusions, comprising:

an analysis engine; and

at least one sensor, configured to communicate with the analysis engine using at least one meta-protocol under which a 4-tuple is used to represent a data item to be sent to the analysis engine for analysis;

wherein the 4-tuple comprises a semantic type, data type, data type size, and value of the data item and represents the data item in a manner that enables the analysis engine to receive and use the data item regardless of how the data item is represented and organized on a platform associated with the sensor;

wherein the at least one sensor is configured to communicate with the analysis engine using a plurality of meta-protocols;

wherein each of the plurality of meta-protocols includes a said 4-tuple;

wherein the analysis engine is configured to invoke the at least one sensor and specify a set of meta-protocols supported by the analysis engine, and wherein the at least one sensor is configured to select a meta-protocol from the set;

wherein the analysis engine is configured to load a rule set while the analysis engine is in operation.

9. The system as recited in claim 1, wherein the set is a null set, and the at least one sensor is configured to use a default protocol.

10. The system as recited in claim 1, wherein the analysis engine is configured to specify a set of semantic codes representing data being requested by the analysis engine.

22. A method for detecting intrusions, comprising the steps of:

providing an analysis engine;

providing at least one sensor; and

defining a meta-protocol including a 4-tuple for communication between the analysis engine and the at least one sensor;

wherein the 4-tuple comprises a semantic type, data type, data type size, and value of the data item and represents the data item in a manner that enables the analysis engine to receive and use the data item regardless of how the data item is represented and organized on a platform associated with the sensor;

wherein the at least one sensor is configured to communicate with the analysis engine using a plurality of meta-protocols;

wherein each of the plurality of meta-protocols includes a said 4-tuple;

wherein the analysis engine is configured to invoke the at least one sensor and specify a set of meta-protocols supported by the analysis engine, and wherein the at least one sensor is configured to select a meta-protocol from the set;

wherein the analysis engine is configured to load a rule set while the analysis engine is in operation.

23. A computer program product for detecting intrusions on a host, the computer program product being embodied in a computer readable medium having machine readable code embodied therein for performing the steps of:

providing an analysis engine;

providing at least one sensor; and

defining a meta-protocol including a 4-tuple for communication between the analysis engine and the at least one sensor;

wherein the 4-tuple comprises a semantic type, data type, data type size, and value of the data item and represents the data item in a manner that enables the analysis engine to receive and use the data item regardless of how the data item is represented and organized on a platform associated with the sensor;

wherein the at least one sensor is configured to communicate with the analysis engine using a plurality of meta-protocols;

wherein each of the plurality of meta-protocols includes a said 4-tuple;

wherein the analysis engine is configured to invoke the at least one sensor and specify a set of meta-protocols supported by the analysis engine, and wherein the at least one sensor is configured to select a meta-protocol from the set;

wherein the analysis engine is configured to load a rule set while the analysis engine is in operation.

2. Cancel claims 6,7,8,18.

Examiner's Statement of Reasons for Allowance

3. Claims 1,2,5,9-17 and 19-23 are allowed over prior art.

4. This action is in reply to applicant's correspondence of 21 October 2004.

5. The following is an examiner's statement of reasons for the indication of allowable claimed subject matter.

6. As per claims 1,22,23, prior art of record, Maloney et al, U.S. Patent 6,269,447 B1 fails to teach, alone, or in combination, of (as shown for claim 1 by example);

(claim 1) A system for detecting intrusions, comprising:

an *analysis engine*; and

at *least one sensor*, configured to communicate with the analysis engine using at least one meta-protocol under which a 4-tuple is used to represent a data item to be sent to the analysis engine for analysis;

wherein the *4-tuple comprises a semantic type, data type, data type size, and value of the data item and represents the data item in a manner that enables the analysis engine to receive and use the data item regardless of how the data item is represented and organized on a platform associated with the sensor*;

wherein the at least one sensor is configured to communicate with the analysis engine using a *plurality of meta-protocols*;

wherein *each* of the plurality of *meta-protocols includes a said 4-tuple*;

wherein the analysis engine is configured to invoke the at least one sensor and *specify a set of meta-protocols* supported by the analysis engine, and wherein the at least one sensor is configured to *select a meta-protocol from the set*;

wherein the analysis engine is configured to *load a rule set while the analysis engine is in operation*.

7. The italicized above claim elements dealing with (for example; claim 1) "A system for detecting intrusions, comprising: ... *analysis engine*; ... *least one sensor*, ... *4-tuple comprises a semantic type, data type, data type size, and value of the data item and represents the data item in a manner that enables the analysis engine to receive and use the data item regardless of how the data item is represented and organized on a platform associated with the sensor*; ... *plurality of meta-protocols*;... *meta-protocols includes a said 4-tuple*; ... *specify a set of meta-protocols*

... select a meta-protocol from the set;... load a rule set while the analysis engine is in operation... " serving to patently distinguish the invention from prior art. Specifically, the use of an integrated analysis engine with at least one sensor as applied to the intrusion detection (network/inter-networked) environment, per se, is known in the prior art.

However, as per the applicants arguments in the previous remarks in the Amendment (October 21, 2004), the examiner finds the applicant's arguments to be persuasive in that, the utilization of a communications protocol, and more specifically at the meta-protocol level of abstraction, whereas the said meta-protocol is explicitly defined in the claim language to comprise "[a] 4-tuple [that] comprises a semantic type, data type, data type size, and value of the data item and represents the data item in a manner that enables the analysis engine to receive and use the data item regardless of how the data item is represented and organized on a platform associated with the sensor". These aspects in terms of such specificity serving to patently distinguish the invention from the prior art of record.

Further, the use of a common (i.e., at the "Meta" level of abstraction) language for communications of intrusion events/detection/logging/analysis (i.e., see Undercoffer, J., et al, "Modeling Computer Attacks: A Target-Centric Ontology for Intrusion Detection", Dept. of CS & EE, University of Maryland Baltimore County, 2002, "http://www.csee.umbc.edu/cadip/2002Symposium/Ont-for-IDS.pdf", entire document), although by itself a characteristic of the applicant's inventive concept, is in no way obviously associated with any given multi-sensor IDS system, nor is any specific description of the "4-tuple" mentioned, implicitly or explicitly. Also, the use of virtual machine/object technologies as applied to creating IDS's with generic interfaces for multi-purpose monitoring applications (see Al-Shar, E., et al, "HiFi+: A Monitoring Virtual Machine for Autonomic Distributed Management", School of CS, DePaul Univ., 2004, "http://www.mnlab.cs.depaul.edu/~ehab/papers/dsom04.pdf, entire document"),

more addresses the multi-IDS's aspect of the applicants inventive concept, the teachings likewise is in no way obviously associated with any specific description of the "4-tuple" mentioned, implicitly or explicitly.

However, the claim language (at least insofar as independent claims 1,22,23 are concerned) clearly and explicitly relates the "4-tuple" protocol to an explicit combination of data items/data types to form a inter/intra communications protocol for the analysis engine and sensors, that is a central aspect of the multi-sensor architecture that the invention is concerned with.

8. Claims 22,23 deal with method, software embodiment variations for the system of claim 1. These claims clearly encompass the inventive aspects of the claim 1 limitations across various claim 1 alternative embodiments, and are allowable on a similar basis.

9. Dependent claims 1,2,5,9-17 and 19-21 are allowable by virtue of their dependencies.

Conclusion

10. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3681, and whose unofficial Fax number is (571) 273-3681. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization where this application is assigned is 703-872-9306.

Ronald Baum

Patent Examiner